БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ
ИНСТИТУТ ПО ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ ТЕХНОЛОГИИ

Тодор Велев Велев

МОДЕЛИРАНЕ И АВТОМАТИЗАЦИЯ НА СТАНДАРТИЗИРАНИ СИСТЕМИ ЗА УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА

АВТОРЕФЕРАТ

на дисертация

за придобиване на образователната и научна степен „доктор“
по докторска програма научна специалност „Информатика”
професионално направление 4.6 Информатика и компютърни науки

Научен ръководител: **проф. д-р Нина Добринкова**

София, 2025 г.

Дисертацията е обсъдена и допусната до защита на разширено заседание на секция "Моделиране и оптимизация" на ИИКТ-БАН, състояло се на .....2025 г.

Дисертационният труд е структуриран в увод, три основни глави, основни изводи и заключения, приложения, и изчерпателен списък с използвана литература. Общият обем на дисертацията без приложенията е 124 страници, което включва богато илюстративно съдържание от 29 фигури (диаграми, схеми, екранни изгледи) и 34 таблици, представящи данни и класификации. Списъкът с използваната литература съдържа 80 източника, демонстриращи широтата и задълбочеността на извършения литературен обзор.

Защитата на дисертацията ще се състои на ……г. от …… часа в зала …… на блок …… на ИИКТ-БАН на открито заседание на научно жури в състав:

1. …….
2. .....
3. .....
4. .....
5. .....

Резервни членове:

1. .....
2. .....

Материалите по защитата са на разположение на интересуващите се в стая …. на ИИКТ-БАН, ул. "Акад. Г. Бончев", бл. …..

Автор: Тодор Велев Велев
Заглавие: МОДЕЛИРАНЕ И АВТОМАТИЗАЦИЯ НА СТАНДАРТИЗИРАНИ СИСТЕМИ ЗА УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА

I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИЯТА

Актуалност на проблема

В съвременната информационна действителност, характеризираща се с динамична цифровизация на всички обществени и икономически процеси, информацията се превръща в стратегически актив и в същото време – във все по-уязвим ресурс. Ежедневният обмен на огромни масиви от данни, сложната инфраструктура от взаимосвързани системи и повсеместното използване на облачни технологии и мобилни устройства водят до нарастване на заплахите за сигурността на информацията. Зачестяват кибератаките, инцидентите с неоторизиран достъп и компрометиране на данни, което поставя предизвикателства пред организациите, както в публичния, така и в частния сектор.

Традиционните подходи към сигурността, базирани предимно на ръчни процеси, отделни технически средства или формално изпълнение на минимални изисквания, вече не отговарят на актуалните рискове. На този фон международните стандарти, като ISO/IEC 27001, NIST, FISMA, GDPR и други, изискват системен, интегриран и адаптивен подход към управлението на информационната сигурност. Те предполагат изграждане на системи за управление на сигурността на информацията (СУСИ), които съчетават политики, процедури, технологии, човешки фактор и организационна култура.

Автоматизацията на процесите в СУСИ е нова необходимост, предопределена от сложността и обема на данните и информационните потоци. Дигиталните платформи за управление на СУСИ трябва да осигуряват проследимост, контрол, непрекъсната оценка и подобрение, както и възможност за интеграция с нови нормативни изисквания и бизнес промени. В тази динамична среда информационната сигурност е задача с висок приоритет и нарастващо значение. Системите за управление на информационната сигурност не са адекватни без автоматизирани платформи с елементи на изкуствен интелект, които да овладеят нарастващите по обем и видове информационни потоци и взаимодействия.

Актуалността на настоящия дисертационен труд произтича от ясно идентифицирана необходимост от нов, качествено различен подход към управлението на стандартизирани СУСИ. Този подход трябва да се основава на формализиран, смислово богат модел на областта на сигурността и да използва този модел за постигане на висока степен на автоматизация на процесите. Разработването на интелигентна, интегрирана програмна среда (платформа), базирана на такъв модел, може драстично да повиши резултатността, ефикасността и приспособимостта на управлението на сигурността, като същевременно намали разходите и административната тежест върху организациите.

Обект и предмет на изследването

Обектът на изследване са стандартизираните системи за управление на сигурността на информацията (СУСИ) и възможностите за автоматизация на функционалностите и управлението им.

Предмет на изследване е Модел на програмен продукт комплексна Платформа, която да моделира и автоматизира произволна система за управление на сигурността на информацията, изградена в съответствие с международно признат стандарт или стандарти в тази област.

Цели и задачи

Целта на дисертационната работа е да разработи и апробира модел на платформа, която да управлява и автоматизира стандартизирани системи за управление на сигурността на информацията.

За реализиране на тази цел са формулирани следните задачи:

- Изследване и анализ на теоретичните основи на стандартизирани системи за управление на сигурността на информацията в аспекти:
  - Сигурност на информацията;
  - Стандарти за информационна сигурност;
  - Системи за управление на сигурността на информацията СУСИ;
  - Софтуерните приложения за ИС.

- Анализ на процесите, изискванията и характеристиките на платформата за управление и автоматизация на стандартизирани системи за управление на сигурността на информацията. Задачата е разделена в съответствие с посочената методика на следните подзадачи:
  - Изследване и анализ на работни процеси, подлежащи на автоматизация и съответстващите им информационните потоци;
  - Определяне на функционалните и нефункционалните изисквания на платформата, чрез изследване и анализ на данните, на потребителските групи и на стандартите за информационна сигурност;
  - Идентифициране на общите характеристики на системата.
- Проектиране на оптимален модел на платформа за моделиране и автоматизация на стандартизирани системи за управление на сигурността на информацията и прилежащата му архитектура.

Методи

За постигането на поставените цели и задачи в дисертационния труд е използвана комбинация от научноизследователски методи, осигуряващи както теоретична задълбоченост, така и практическа приложимост на резултатите.

- **Системен анализ**

Този метод е приложен за разглеждане на СУСИ като комплексна, динамична система от взаимосвързани компоненти, процеси и дейности. Чрез системния анализ са идентифицирани основните елементи на СУСИ, техните зависимости, входни и изходни параметри, както и взаимодействието им с външната среда на организацията. Системният подход позволи структурирането на проблема, декомпозирането му на по-малки, управляеми части и интегрирането им в единен модел на платформа.

- **Сравнителен анализ**

Извършен е задълбочен сравнителен анализ на различни международни стандарти (ISO/IEC 27001, ISO/IEC 27002, NIST Cybersecurity Framework), регулаторни изисквания (GDPR, NIS2), методологии за управление на риска (ISO 31000) и съществуващи софтуерни решения за СУСИ. Този анализ позволи идентифицирането на добри практики, общи елементи и пропуски в текущите подходи, което послужи като основа за формулиране на изискванията към новата платформа.

- **Моделиране**

Методът на моделирането е централен за дисертацията. Използвани са следните техники:

  - Концептуално моделиране - за дефиниране на високо ниво на компонентите и логическата структура на предложената платформа;
  - Архитектурно моделиране - за проектиране на софтуерната архитектура, включително избор на слоеве, модули и технологичен стек;

- Моделиране на бизнес процеси (BPMN - Business Process Model and Notation) - използван е за детайлно описание на ключови процеси в СУСИ (напр. оценка на риска, управление на инциденти, одит) с цел тяхната стандартизация и подготовка за автоматизация;
- Моделиране на данни (ERD - Entity-Relationship Diagram) - приложен е за структуриране на информацията, дефиниране на обекти, техните атрибути и взаимовръзки, необходими за базата данни на платформата.

- **Анализ на данни**

Използван за събиране, систематизиране, обработка и интерпретиране на информация, свързана със статистически данни за киберзаплахи, ефективност на съществуващи мерки за сигурност, както и данни, генерирани по време на тестове на прототипа.

- **Литературен обзор**

Извършен е задълбочен и систематичен преглед на научна и професионална литература – книги, научни статии, конференции, доклади, стандарти и добри практики в областите на информационната сигурност, системите за управление, моделирането на процеси, софтуерното инженерство и автоматизацията.

- **Метод на експертните оценки**

При дефинирането на изискванията и валидацията на модела и прототипа, индиректно са взети предвид експертни

мнения и препоръки от специалисти в областта на информационната сигурност и одита.

Комбинацията от тези методи осигурява всеобхватен подход към проблема, съчетавайки теоретичното познание с практическото приложение и валидация на предложените решения.

II. ОБЕМ И СТРУКТУРА

Дисертационният труд е систематично организиран в увод, три основни глави, основни изводи и заключения, приложения, и изчерпателен списък с използвана литература. Общият обем на дисертацията без приложенията е 124 страници, което включва богато илюстративно съдържание от 29 фигури (диаграми, схеми, екранни изгледи) и 34 таблици, представящи данни и класификации. Списъкът с използваната литература съдържа 80 източника, демонстриращи широтата и задълбочеността на извършения литературен обзор.

III. СЪДЪРЖАНИЕ НА ДИСЕРТАЦИЯТА

Увод

В увода е изяснена актуалността на проблема и са представени методическите параметри на дисертационния труд, структурата, обектът, предметът, целите и задачите.

ГЛАВА 1 Стандартизирани системи за управление на сигурността на информацията

Първа глава на дисертационния труд има за цел да положи теоретичните основи на изследването. Тя извършва подробен преглед и анализ на съществуващите подходи, стандарти и технологии в областта на управлението на сигурността на информацията. Главата е структурирана така, че да изведе систематично проблемите и пропуските, които настоящата работа цели да разреши.

Направен е теоретичен анализ на фундаменталните постаменти върху които се изгражда модела на Платформата за управление и автоматизация на стандартизирани системи за управление на сигурността на информацията, а именно: Сигурност на информацията; Стандарти за информационна сигурност; Системи за управление на сигурността на информацията СУСИ; и Софтуерни приложения за ИС.

В главата са дефинирани терминологията и аспектите на информационната сигурност, методите, технологиите и инструментите за защита на информацията и предизвикателствата, провокиращи изследването. Обсъжда се еволюцията на информационната сигурност от чисто технически аспект до всеобхватен управленски процес. Представя се необходимостта от систематичен подход за управление на сигурността в организациите, който да излезе извън рамките на конкретните мерки и да осигури дългосрочна устойчивост. Анализирани са стандартите за информационна сигурност, както и терминологията, същността и целите на

стандартизацията. Разглежда се историческото развитие на стандартите за информационна сигурност, като се започне от ранни инициативи до формирането на международни рамки. Обсъждат се ползите от внедряването на стандартизирани СУСИ, включително подобряване на управленските процеси, намаляване на риска, повишаване на доверието на клиенти и партньори, и спазване на регулаторни изисквания

Изследвани са основните елементи, архитектурата и процесите по разработка и внедряване на СУСИ. Тази секция прави детайлен преглед като се описват ключовите елементи на СУСИ съгласно стандарта, включително:

- Контекст на организацията - разбиране на вътрешни и външни проблеми, заинтересовани страни и обхват на СУСИ;
- Лидерство - ангажираност на висшето ръководство, политики и разпределение на роли и отговорности;
- Планиране - адресиране на рискове и възможности, цели за сигурност и планове за постигането им;
- Поддръжка - ресурси, компетентност, осведоменост, комуникация и документирана информация;
- Оперативна дейност - оперативно планиране и контрол, оценка на риска за информационната сигурност, обработка на риска за информационната сигурност;
- Оценка на изпълнението - мониторинг, измерване, анализ, оценка, вътрешен одит и преглед от ръководството;
- Подобрение - несъответствия и коригиращи действия, и

непрекъснато подобрение. Специално внимание се обръща на Приложение А на ISO/IEC 27001, което съдържа списък с контроли за сигурност, категоризирани по домейни.

Въпреки значителните ползи, внедряването и поддържането на СУСИ е свързано с редица предизвикателства. Анализират се трудностите, които често водят до забавяне, повишени разходи или неуспешно сертифициране. Обсъждат се:

- Липса на ресурси - недостатъчен персонал, бюджет и време;
- Сложност на процесите - голям брой документи, процедури и контролни точки;
- Съпротивление на промяна - трудности при промяна на културата и работните навици в организацията;
- Управление на документацията - обемна и динамична документация, която изисква постоянно актуализиране;
- Одит и съответствие - сложни процеси за вътрешен и външен одит, изискващи изчерпателни доказателства за съответствие;
- Непрекъснато подобрение - поддържане на СУСИ в постоянно съответствие с променящите се заплахи и бизнес нужди.

Тези предизвикателства служат като основа за аргументиране на необходимостта от автоматизация и моделиране, които да адресират тези проблеми.

В първа глава се анализира също и пазара на софтуерни инструменти за подпомагане на СУСИ. Проучени са функционалностите на водещи продукти и са идентифицирани следните общи недостатъци:

- Ориентация към пасивна документация - повечето системи са "електронни хранилища" за съхранение на политики, процедури и записи. Те подпомагат одита, но не и активното, динамично управление.
- Липса на смислово разбиране - данните се съхраняват в релационни бази данни, които не управляват сложните семантични връзки между активи, заплахи, контроли и бизнес процеси. Това ограничава възможностите за автоматизирани анализи и изводи.
- Слаба автоматизация на процесите - процеси като оценката на риска често се свеждат до попълване на електронни таблици, които след това се качват в системата. Липсва истинска автоматизация, базирана на логически правила.
- Ниска гъвкавост и разширяемост - системите обикновено са изградени около един конкретен стандарт и трудно се адаптират към други рамки или специфични за организацията изисквания.

Основни изводи към Глава 1

☞ Въз основа на направения анализ на сигурността на информацията, стандартите за информационна сигурност и системите за управление на сигурността на информацията се налага извода, че е необходим комплексен подход за справяне с описаните прогресиращи предизвикателства.

- От изследването на видовете и функционалния обхват на софтуерните приложения, свързани със СУСИ се идентифицира сегментацията на продуктите. Системите за цялостно управление на СУСИ са предимно в аспекти сертификация, ре сертификация и поддържане на необходимите записи и шаблони за целите на одитния процес. Липсват цялостни решения които да управляват и контролират всички работни процеси и информационни потоци в инфраструктурата и суперструктурата на организацията. Платформения подход за изграждане на адаптивна система, моделираща и автоматизираща стандартизирани системи за управление на сигурността на информацията е иновативно, генерализирано решение на третираната проблематика.
- С цел да се гарантира ефективност, полезност и надеждност на платформата е необходимо да се разработи модел, който се базира на цялостен мониторинг, анализ и управление на документната матрица, работните процеси и информационните потоци и активи на организацията.

ГЛАВА 2. Моделиране на платформа за управление и автоматизация на стандартизирани системи за управление на сигурността на информацията.

Във Втора глава е представена методология за изследване и моделиране на автоматизирана стандартизирана платформа за управление на сигурността на информацията и съобразно нея е извършен анализ на процесите, определяне на изискванията и идентифициране на общите характеристики на системата.

Изследването и анализа, съобразно предложената методология включва следните ключови стъпки:

- **Анализ на процесите**

Изследване и анализиране на стандартизираните работни процеси, които системата да автоматизира и кореспондиращите с тях информационните потоци.

Идентифицирани и описани са следните стандартизирани работни процеси:

- Изпълнение на бизнес процеси ИБП/Документооборот ;
- Процеси по администрация на платформата;
- Дефиниране и управление на бизнес процеси;
- Управление на СУСИ;
- Мониторинг и контрол;
- Одит.

- **Определяне на изискванията**

За определяне на функционалните и нефункционалните изисквания се извърши:

- Изследване и анализ на потребителските групи;

Потребителите на платформа за управление и автоматизация на стандартизирани системи за управление на сигурността на информацията са обособени в 2 големи групи:

- Ползватели - компании и организации внедрили Система за управление на информационната сигурност, сертифицирана по международно признат стандарт.

Това са ползватели от всички сектори на икономиката, изпълняващи дейност във всички раздели на класификатора на икономическите дейности, включително държавни и общински организации.

- Сертификационни и консултантски организации - извършват одити при сертифицирането на СУСИ и контролни одити за потвърждаване на съответствието.

  - Изследване и анализ на стандартите за информационна сигурност;

Изследването на изискванията на стандартите се извърши съобразно техните основни групи характеристики:

- Съдържание на стандарта - име, цел, политики, обхват, изисквания, условия, определения, вид и област на приложимост.
- Инфраструктура - процедури, процеси, документи, контроли, регистри, срокове, инструменти и функционални алгоритми.
- Суперструктура (външна среда) - кореспонденти, клиенти, доставчици, партньори и институции, свързани стандарти, възможни възможности за интеграция, одити, и т.н.
- Ресурси - организационна структура и персонал, активи, инструменти и материали, необходими за планиране, поддържане и контрол на стандартните механизми.

  - Изследване и анализ на данните.

Платформа за управление и автоматизация на стандартизирани системи за управление на сигурността на информацията СУСИ, оперира с две основни групи данни, като следва:

- Данни свързани със стандартите за информационна сигурност;
- Данни свързани с функционалните изисквания за Платформата;

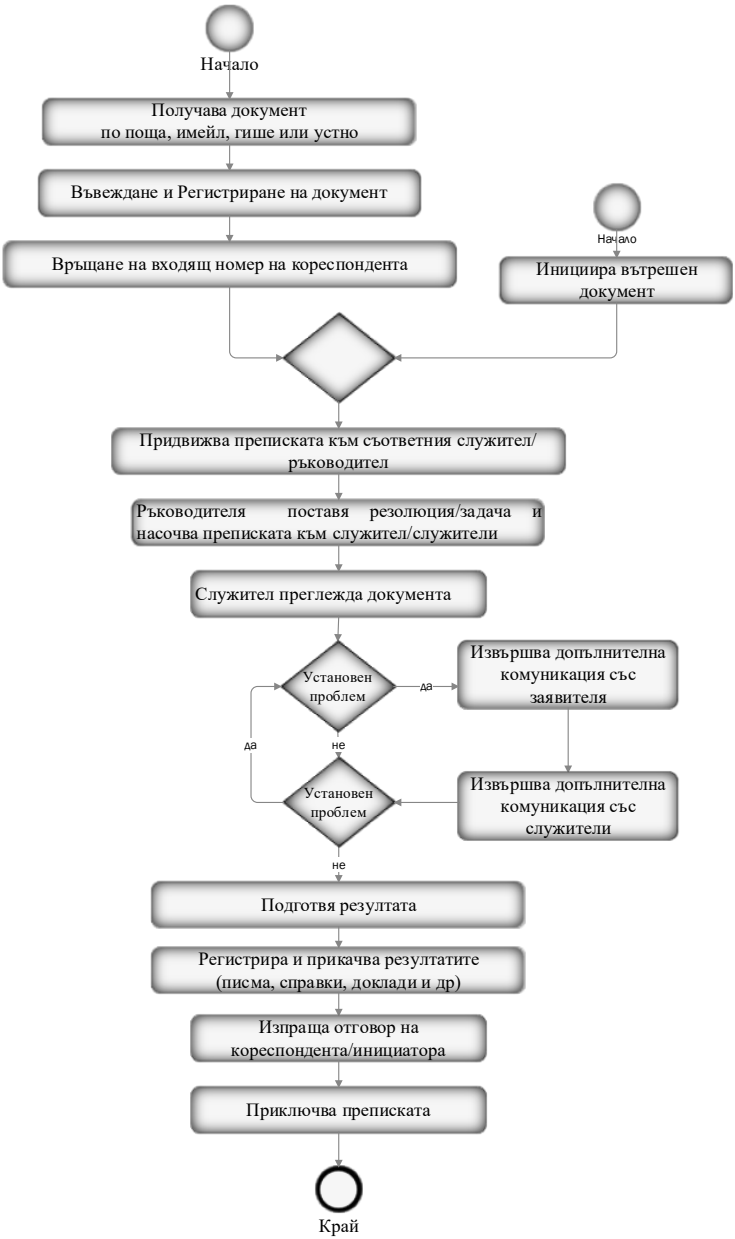
Резултата е показан в Приложение 3.

- **Определяне на общите характеристики на платформата**

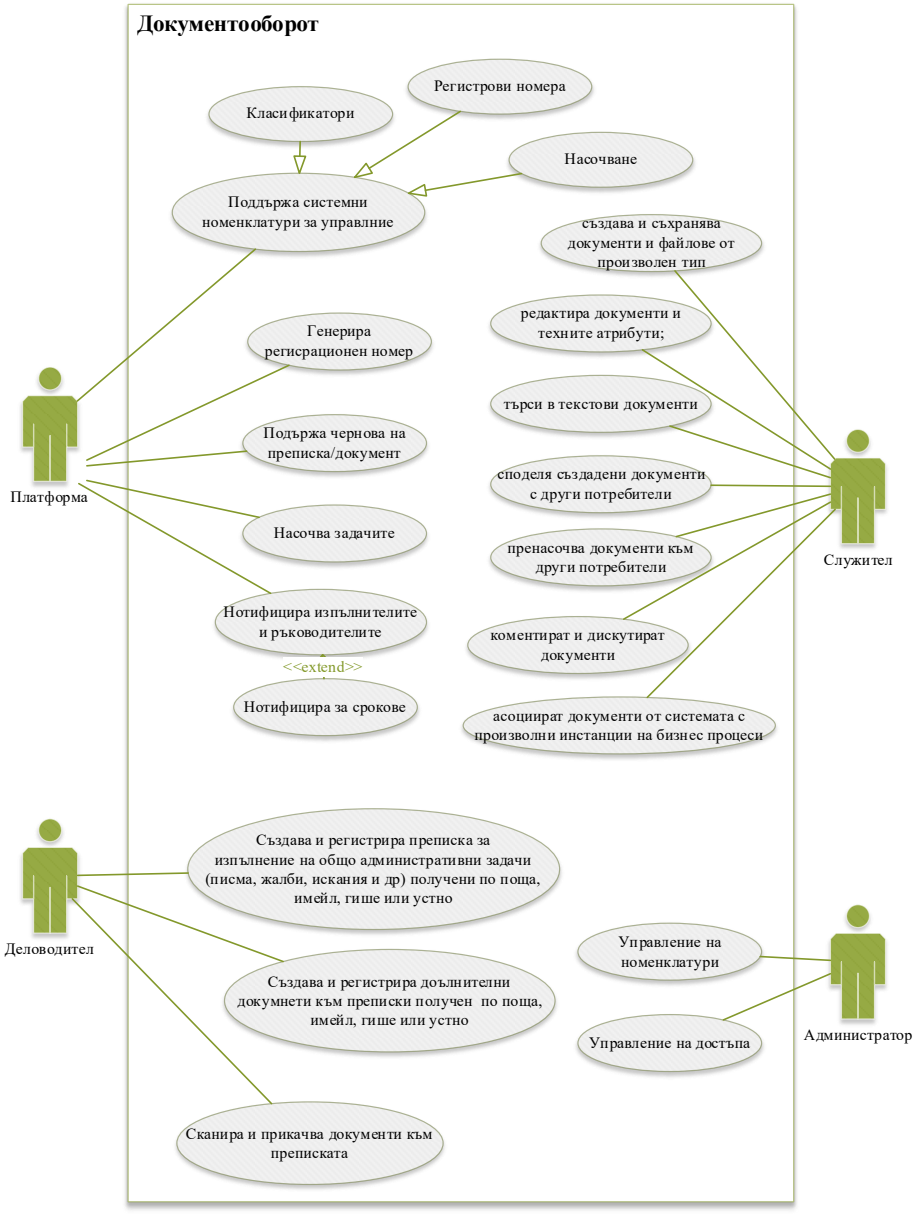
Общите характеристики на платформата са определени чрез изследване на добрите практики за потребителско поведение, продуктивност, сигурност и администрация на информационните системи. Поради спецификата на поставените цели и изучаваната материя за тази задача са използвани евристични техники като:

- Подход най-добри практики;
- Проучване и анализ на академични източници;
- Техника SCAMPER;
- Методът Делфи

За описание на процесите и изискванията е използван е унифицираният език за моделиране – UML™ и Business Process Model and Notation (BPMN) стандарта за визуално моделиране на бизнес процеси под формата на диаграми като показаните по-долу.



Фигура 1 Процес Документооборот



Фигура 2 Документооборот диаграма на потребителските случаи

Основни резултати от Глава 2

- ☞ Извършен е анализ на стандартизираните работни процеси, които да бъдат включени в модела на Платформата, подлежащи на автоматизация и съответните, кореспондиращите с тях информационните потоци.
- ☞ Въз основа на анализ на данните, на потребителските групи и на стандартите за информационна сигурност са определени функционалните и нефункционалните изисквания, които трябва да бъдат отразени при моделирането на Платформата.
- ☞ Изследвани са добрите практики за потребителско поведение, продуктивност, сигурност и администрация на информационните системи и са идентифицирани общите характеристики на Платформата.

ГЛАВА 3. Модел на платформа за моделиране и автоматизация на стандартизирани системи за управление на сигурността на информацията.

В трета глава е представена авторската теория за документна матрица, като основа за оперативно управление на организация и компанията. Описаната е методиката за моделиране и концептуалният модел на Платформата. Изработен е оптимизиран модел на предмета на дисертацията, изграден съобразно теоретичните постаменти и направените изследвания и анализи, представени в Глава 1 и Глава 2. Предложена е логическа и физическа архитектура за реализация на платформата.

Документна матрица

Всяка компания независимо от мащаба си изпълнява своята дейност във вътрешна и външна работна среда. Вътрешната среда се определя от ресурсите на компанията (човешки, материални и нематериални) и от работните процеси в нея, свързани с предмета на дейност. Външната среда са клиентите, доставчиците, партньорите и държавните институции с които компанията работи.

Системите за управление на сигурността на информацията по международно признатите стандарти дефинират, регламентират, управляват, наблюдават, регистрират и архивират вътрешната и външната среда на функциониране, чрез системата от документи на организацията и кореспондиращите масиви от данни.

Документа е запис, чрез който се отразява в неговото развитие всяко действие, норма, събитие, ресурс, отношение, процес и интелектуално производство. Освен че в днешно време документите са електронни и хартиени те могат условно да се класифицират в няколко формални групи - Конвенционални записи и Специализирани документи

Количеството от всички тези записи, наречени документи, дефинират и определят компанията, нейната история, капацитет, качество и конкурентно способност.

Документите сами по себе си не са независими отделни единици. Те са свързани в специфична за всяка фирма **документна мрежа**. Всеки документ е краен продукт, зад който

стои процес от различна сложност и обхват. Всеки документен процес се състои от дейности и етапи и както във всяко производство се нуждае от ресурси и материали. Ресурсите и материалите от своя страна са най-често масиви от данни и други документи, които имат своите процеси и своя жизнен цикъл. Множеството документи и връзките между тях образуват документната мрежа на организацията. За разлика от Интернет мрежата обаче документната мрежа на една компания има дефинирани пътища, връзки и форми (формуляри) и е свързана и индексира и управлява масивите (базите) от данни на организацията.

По тази причина системата от фирмени документи се разглежда не като документната мрежа, **а като документна матрица** на компанията.

Документната матрица засяга всеки елемент от вътрешната и външна работна среда на фирмата и е съвсем логично тя да дава възможност за максимален контрол върху организацията. Фирмената документна матрица е в основата на управлението на всяка система за управление, изградена по международно признати стандарти. Те са базирани на политики, работни процеси, процедури и множество форми и записи за контрола им.

Когато документите се цифровизират, връзките между тях се визуализират и матрицата се облече в подходяща функционалност, то се получава изключително ефективна система за мониторинг, контрол и управление на всички нива и ресурси в компанията.

Концепция на платформата

Платформата за моделиране и автоматизация на стандартизирани системи за управление на сигурността на информацията е съвременна, иновативна, интегрирана информационно-оперативна система, която моделира, дигитализира, регистрира, управлява, съхранява и контролира работните процеси и свързаната с тях информация и документация в съответствие с различни международно признати стандарти за информационна сигурност.

Модела се базира на мониторинг, анализ и управление на документната матрица, работните процеси и на информационните потоци и активи на организацията. Платформата обхваща всички информационни единици - документи (хартиени и електронни), аудио и видео комуникации, системни, програмни и комуникационни логове и др.. Мониторира входящите, изходящите и вътрешните информационни потоци и ги управлява, съобразно моделираните в нея работни процеси и стандартизирани форми.

Работните процеси и стандартизираните форми са моделирани, съобразно политиките, процедурите и шаблоните на системите за управление на сигурността на информацията (СУСИ). Всички записи, свързани не само с елементите на СУСИ, а и с оперативните процеси се формализират във платформата и се извършват само чрез нея. Целта е да се използват най-новите технологични постижения, за да се цифровизира, индексира и съживи документната матрица на

организацията и да позволи оперативна ефективност на управление на сигурността.

Информационните активи се въвеждат в Платформата като параметризирани обекти. Всеки контрол от системата от контроли на стандартите за информационна сигурност, съобразно които е изградена СУСИ се асоциират с един или няколко предварително дефинирани критерия на платформата. Всеки критерий е формализиран запис с определени параметри на регистрираната информация и честота и начин на проверка. За всеки критерий се дефинират тригери на действие на платформата, съобразно възможни стойности или събития.

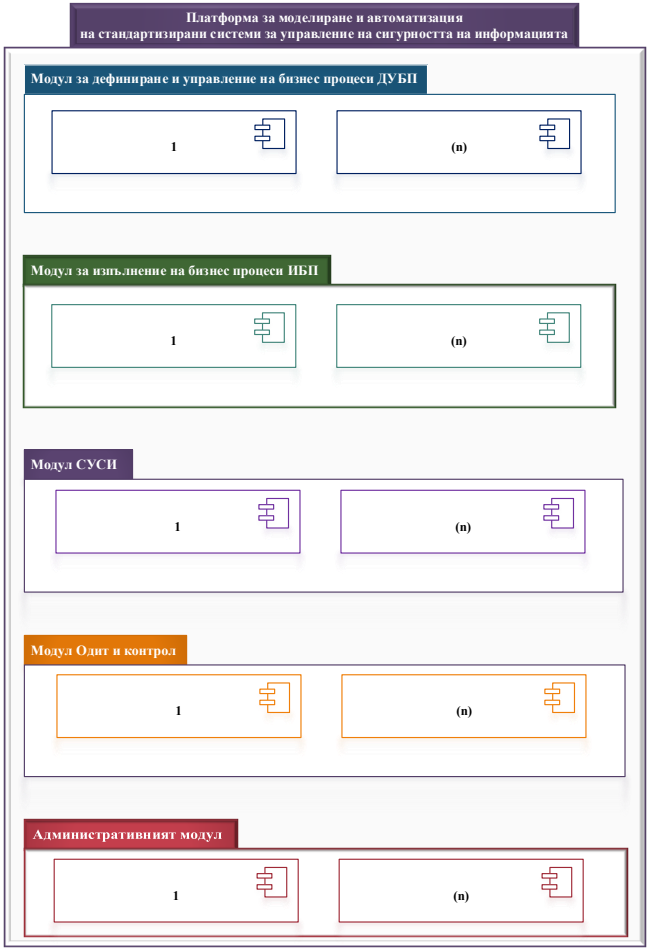
Контролите се прилагат към актив и/или процес в съответствие със СУСИ.

Мисията на платформата е да интегрира всички документи потоци, свързани с работните процеси в клиентската организация. Да свърже множеството приложни софтуерни продукти, работещи в сферата на информационната сигурност и масивите от данни в една единна информационно-комуникационна и управленска система. Платформата обединява информационните сечения и информационните потоци в единно информационно пространство и осигурява интегрирана среда за съхранение, управление и обмен. Това позволява да се следи ефективно движението на информацията, структурирана в отделни типове документни единици, да се моделира СУСИ и да се осъществява надежден контрол.

Платформата моделира йерархичната структура на организацията, с възможност за изменения, като позволява адекватно разпределение на задачите съобразно субординацията на компанията. Системата управлява движението на разнообразни типове документи, като автоматизира всички фази на работните потоци.

Съгласно извършените изследвания и анализи, представени в Глава 2 Платформата за моделиране и автоматизация на стандартизирани системи за управление на сигурността на информацията се реализира със следните компоненти (модули):

- Модул за дефиниране и управление на бизнес процеси ДУБП;
- Модул за изпълнение на бизнес процеси ИБП;
- Модул СУСИ;
- Модул Одит и контрол;
- Административният модул;



Фигура 3 Структура на Платформата

Платформата използва единна база от данни в която чрез различни интерфейси се въвежда и извежда необходимата информация, съобразно информационните класове. Базовите масиви се управляват чрез изграждане на специализирана логика за всеки от тях – стандарти, термини, процеси,

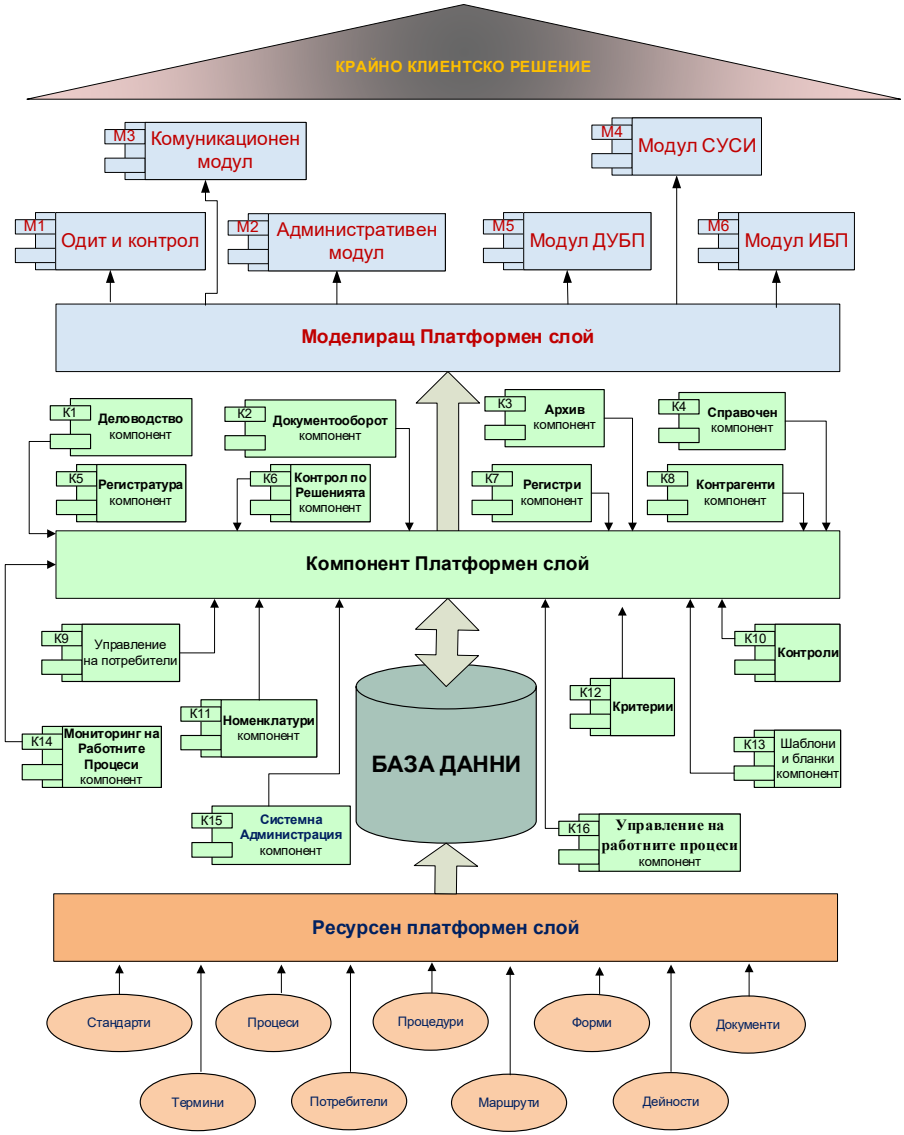
потребители, процедури, маршрути, форми, контролирани процеси, и различни неструктурирани данни.

Платформения слой, така наречения мидълуер, реализира логиката и обмена на информация между интерфейсите за въвеждане на информация и базата от данни. Друг платформен слой, реализира връзката на функционалните модули и базата от данни. Функционалните модули (компоненти) изпълняват определена група от функции, чрез предоставяне на интерфейси за осъществяване на необходимите задачи. Платформата изгражда модулите си в контекста на всяка клиентска организация, като набор от компоненти (функционални модули) както е показано на фигурата.

Системата притежава регистрационно-контролна част, в която се въвеждат индекси на организацията и се регистрират в съответствие с тях всички входящо-изходящи и вътрешно оперативни документи (събития). Автоматично се генерират номера на документите съгласно предварително заложен стереотип. Към всеки регистриран документ могат да се задават срокове за изпълнение, които тя контролира. Платформата функционира и като комуникатор, като информира по различни начини (е-мейл, SMS, звуково и визуално) за различни контролирани събития, просрочени срокове и задачи за изпълнение. Електронната система моделира създадените в компанията по съответния стандарт оперативни процедури и процесни карти, като осигурява информационно коректното спазване на всички работни процеси, попълване на съответните

формуляри и бланки, мониторинг на работните процеси и контрол на решенията. Тя гарантира възможно най-високи нива на сигурност, надеждност и защита на информацията. Осигурява възможност всеки потребител да се идентифицира не само с потребителско име и парола, а и с частен електронен подпис. Всеки служител/потребител има предварително дефинирани профили, роли, права на достъп и функционалност, съответстваща на длъжностната му характеристика. Системата генерира динамично персонални екрани при влизането на потребителя, като му предоставя интуитивен потребителски интерфейс и навигация.

Модулите на Платформата изграждат моделите, свързани с управление на различи типове международно признати стандарти с богат инструментариум: **типизирани процеси**; **предварително разработени сценарии и постановки**; набор от предварително дефинирани форми; разработени конвенционални регистри; специализирани регистри; вътрешна комуникационна среда; системи за оценка, контрол и подпомагане на одита; и други.



Фигура 4 Концептуална архитектура на модела

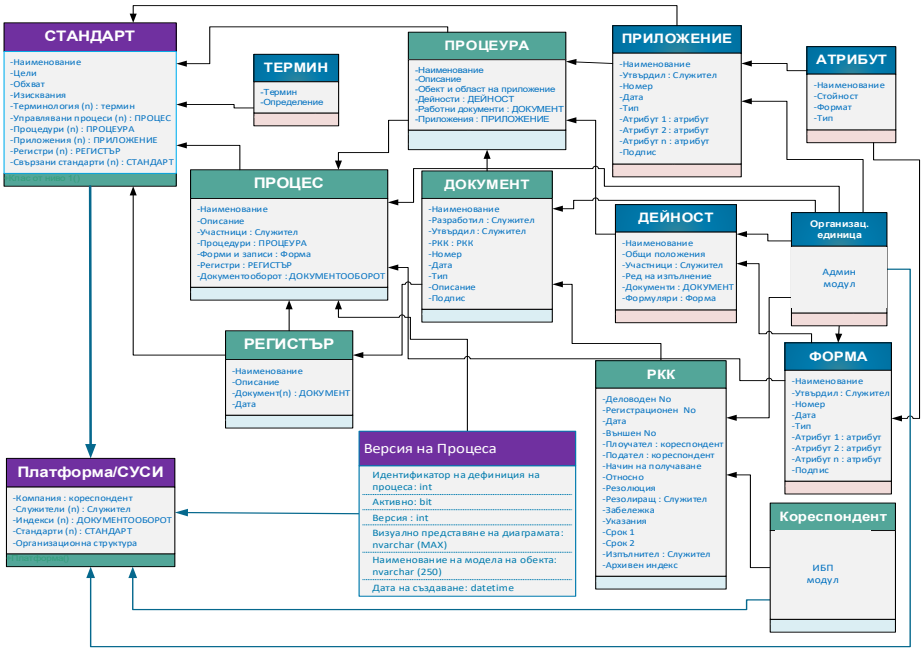
Методика за моделиране

Въз основа на функционални и нефункционални изисквания, бизнес процесите и спецификацията на потребителски случаи, дефинирани в предходната глава след направеното изследване и анализ, се разработи оптимален набор от информационни определители, разпределени в логически информационни класове и подкласове.

Наборът от дескриптори, генериран от извършените изследвания и анализи е декомпозиран на логически информационни класове, в съответствие с тяхната функционална ориентация в описанието на стандартите. Информационните класове се разглеждат като програмни обекти и подобекти. Те се описват чрез своите атрибути, които се наричат информационни идентификатори. Тяхното представяне е унифицирано чрез използване на специфичен технически формат, който определя формата на представяне на стойностите на всеки атрибут на информационните обекти. Техническият формат на информационните класове и техните атрибути се описва от синтаксиса на унифициран език за моделиране (UML).

За дизайна на платформата се използват UML клас диаграми. които изобразяват структурата на системата чрез моделиране на нейните класове, свойства, операции и връзки между обекти. Клас диаграмата е визуална нотация, използвана за изграждане и визуализиране на обектно-ориентирани системи. Тя е статична структурна диаграма, демонстрираща свойствата на платформата, класовете, операциите и връзките

между обекти за описание и дизайн на системата. Диаграмите на класове са форма на структурни диаграми, тъй като те определят какво трябва да бъде включено в моделираната система. Информационните идентификатори са моделирани в 3 нива информационни класове структурирани в модули на платформата. За пример прилагам модел на един основен модул СУСИ.



Фигура 5 Модул СУСИ

Идентификаторите за всеки клас са описани подробно в табличен вид.

Таблица 1 Организационна единица (Структура)

Описание		
Тип	**Наименование/ Формат**	**Описание**
Клас	Организационна единица: () Структура	Организационна единица (Структура) е базов клас на Административния модул, отнасящ се към описване на структурата на организацията и кореспондиращото и моделиране в Платформата.
Атрибут	Наименование: Nvarchar (400)	Наименование на организационната структурна единица.
Атрибут	Тип: Тип	Типът на структурата е предефинирана номенклатура – дирекция, отдел, сектор и длъжност.
клас	Родителска Организационна единица: Структура	Наименование на родителската организационна единица към която принадлежи структурата. (ако има такава)
Подклас	Права (n): Право	Списък от права върху информационните обекти които има организационната единица и всички нейни подструктури. Определят се набор от права за всеки информационен обект от класификатора – Пример: за информационен обект „Регистър на инцидентите“ право на четене, право на регистриране и право на редакция.

Тип	Наименование/ Формат	Описание
Подклас	Шаблони: Шаблон	Шаблоните са набор от права които могат да се прилагат към всеки информационен обект и да се добавят за структурно звено в комплект.
Подклас	Потребители: Потребител (n)	Списък от служители на организацията които са добавени към организационната структура.

Системна архитектура

Платформата за моделиране и автоматизация на стандартизирани системи за управление на сигурността на информацията се реализира като централизирана уеб базирана система с архитектура ориентирана към услугите (SOA), комбинираща в себе си основните модули, които от своя страна използват инфраструктура от стандартизирани услуги за реализация на обработката за конкретните типове информация.

Ориентираната към услуги архитектура (Service-oriented Architecture) е модел, специално предназначен да намали разходите, да увеличи гъвкавостта и да опрости представянето на бизнеса и операциите на различни части от дейността. Основен принцип на SOA е структурирането на бизнес дейностите в услуги, което дава възможност за тяхното бързо идентифициране и преизползване на вече съществуващите функционалности, както и избягване на дублирането им по време на разработка. Стандартизацията на поведението на тези услуги води до ограничаване на неочакваните въздействия при

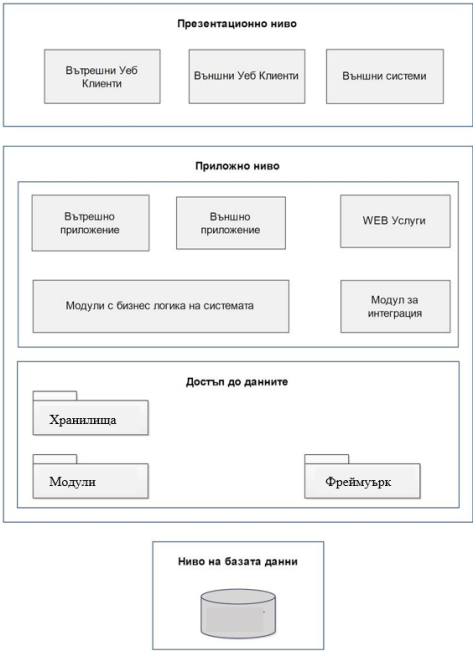
промени, както и до успешното им прогнозиране и избягване. Архитектура ориентирана към услугите (SOA) е съвкупност от независими софтуерни елементи, предоставящи като услуга софтуерна функционалност на други приложения.

Основни предимства на SOA подхода:

- Независимост от доставчик, продукт или технология;
- Услугата е самостоятелна функционална единица.

Услугите могат да бъдат комбинирани с други софтуерни приложения, за да се осигури пълна функционалност на по-голямо софтуерно приложение.

Логическа архитектура



Фигура 6 Системна архитектура на реализацията на Платформата – трислойна архитектура MVC

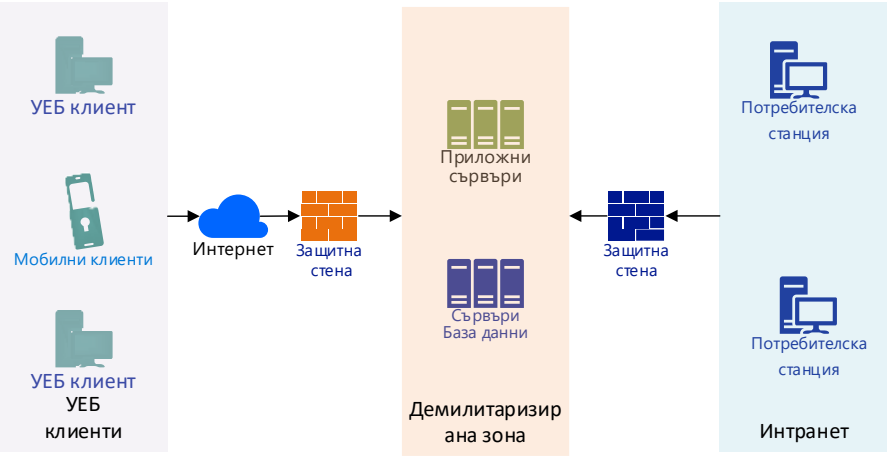
Архитектура на платформата може да бъде декомпозирана на отделни слоеве (нива), комуникиращи помежду си по строго определени интерфейси. Основно предимство при този подход е, че позволява в отделните слоеве да бъдат извършвани значителни промени без това да оказва влияние на останалите, което води до изключителна гъвкавост. Слоевете са определени така, че да групират елементите, които варират независимо. При централизираните платформи доказан модел е разделянето на следните слоеве:

- Слой на базата данни;
- Слой на бизнес логиката;
- Слой на потребителския интерфейс (презентационен слой);

Всеки слой в последствие се декомпозира на отделни модули, като комуникацията между модулите се осъществява по строго специфицирани интерфейси. Разделението на ясно разграничени слоеве и обособяването на слоя на базата данни от слоевете на бизнес логиката позволява да се осигури възможността цялостното решение да бъде съвместимо както със съществуващата инфраструктура в организацията, така и с виртуална инфраструктура.

Физическа архитектура

Платформата се базира на гъвкава архитектура, която ще може да се разгръща както в физическа среда, така и във виртуализирана (облачна) среда, или друго хибридно решение.



Фигура 7 Физическа архитектура

Платформата се адаптира към съществуващата хардуерна, мрежова и приложна среда в организацията, като има два основни физически компонента:

- Приложен сървър, изпълняващ заявките към уеб приложението на системата, чрез който потребителите работят със системата.
- Сървър за управление на базите данни на системата.

Съображенията за максимално добро обособяване и осигуряване на информационна сигурност предопределят отделяне на сървърите в т. нар. DMZ или „демилитаризирана зона“ – зона от мрежата, която е изолирана от останалите части на вътрешната мрежа, отделена от външната среда с външна защитна стена, но и с вътрешна защитна стена, така че евентуален пробив да не доведе до риск за сървъра с приложението на системата или сървъра съхраняващ неговите бази данни.

Основни изводи към Глава 3

- Въвежда се авторската теория за **Документна матрица**, като основа за оперативно управление на компанията и концептуалния модел на Платформата.
- Съобразно описаната методика за моделиране и резултатите от предходните глави е изграден модел на Платформата за моделиране и автоматизация на стандартизирани системи за управление на сигурността на информацията.
- Предложена е логическа и физическа архитектура за реализация на платформата.
- UML кода на модела е представен в **Приложение 5 (Plant UML)**
- Реализацията на Платформата по модули с Python в ООП стил е представено **в Приложение 6.**
- Реализацията на базата данни е дадена в **Приложение 7** ORM (Object-Relational Mapping) реализация чрез (SQL Alchemy стандарт в Python).

IV. ОСНОВНИ ИЗВОДИ И ЗАКЛЮЧЕНИЯ

Научни приноси

- Предложени са алгоритъм и методология за изследване и моделиране на автоматизирана стандартизирана платформа за управление на сигурността на информацията;
- Представена е авторската теория за **документна матрица**, като основа за оперативно управление на организация и компания.

Научно-приложни приноси

- Представен е анализ на системите за управление на сигурността на информацията в аспекти: Сигурността на информацията; Стандартите за информационна сигурност; Системите за управление на сигурността на информацията СУСИ; Софтуерните приложения за ИС.
- Определени, дефинирани и анализирани са работни процеси и потоци, които подлежат на автоматизация чрез разработваната платформа;
- Дефинирани са функционалните и нефункционалните изисквания след извършено изследване и анализ на данните, на потребителските групи и на стандартите за информационна сигурност;
- Идентифицирани са общите характеристики на системата, с използването на евристични методи;
- Разработен е модел на комплексна платформа за

моделиране и автоматизация на стандартизирани системи за управление на сигурността на информацията. Модела се базира на мониторинг, анализ и управление на документната матрица, работните процеси и информационните потоци и активи на организацията.

- Предложена е архитектура на платформата, която е в съответствие със съвременните изисквания за модулност, автоматизация и съвместимост със стандарти.

Насоки за бъдещи изследвания

Постигнатите резултати в дисертационната работа очертават следните насоки за бъдещи изследвания:

- Развитие на Платформата с интеграция с изкуствен интелект, който анализира:
  - Информационните единици и записи;
  - Системните, програмни и комуникационни логове;
  - Информацията генерирана от критериите по контролите.
- Въз основа на извършените анализи с АИ могат да се доразвият функционалностите на платформата в аспекти:
  - Предлагане на оптимизация на СУСИ;
  - Показване на аномалии параметри и активности извън норма;

- Изчисляване на вероятностни събития и предвижда рискови фактори.

- Системите за управление на сигурността на информацията могат да се моделират с невронни мрежи, управлявани от Платформата. Това е подход за повишаване на ефективността и ефикасността на критични системи за управление на информационната сигурност.
- Генеративната неконтролирана невронна мрежа - машина на Болцман (Boltzmann Machine) използва техники върху входните данни за анализиране на нормалните състояния на СУСИ, за да предвиди нежеланите ситуации. Международно признатите стандарти определят набор от контроли за сигурност за наблюдение, одит и управление на СУСИ. Те са разпределени в категории и всяка от тях има стандартизирани атрибути. Невронните единици на машината на Болцман са базирани на инфраструктурата за контрол на сигурността на СУСИ.
- Интегрирането на невронни мрежи в СУСИ може значително да подобри способността на организацията да открива, прогнозира и реагира на аномалии в сигурността. НМ се използват до голяма степен в почти всички области на информационната и киберсигурност, но за моделиране на поведението на СУСИ като цялостна сложна система, те са иновативен метод за намаляване на разходите и времето, както и за предотвратяване или смекчаване на щетите.

Апробация на резултатите

Основните резултати, получени при разработката на дисертационната работа, са докладвани в три публикации и на специализирани международни конференции.

Статии и цитирания

1. Velev T., Dobrinkova N., “Unified innovative Platform for administration and automated management of internationally recognized standards”, Book Title: “Digital Transformation, Cyber Security and Resilience of Modern Societies”, book series “Studies in Big Data”, Springer. DOI:10.1007/978-3-030-65722-2_5, eBook ISBN: 978-3-030-65722-2, ISBN: 978-3-030-65721-5, (https://www.scopus.com/pages/publications/85129091048) ISSN: 2197-6503, 2021, vol. 84, p. 61 – p. 75
2. Velev T, “Heuristic essentials for modeling and optimization of a platform for automation and management of standardized information security management systems”, 28–29 October 2021, Sofia, Bulgaria, 2021 Big Data, Knowledge and Control Systems, Engineering (BdKCSE) IEEE | DOI: 10.1109/BDKCSE53180.2021.9627263, ISBN:978-1-6654-1042-7, https://ieeexplore.ieee.org/document/9627277;
3. Velev T., Dobrinkova N., “The logical model of unify, innovative Platform for Automation and Management of Standards (PAMS)” 1st International Scientific Conference Digital Transformation, Cyber Security and Resilience" DIGILIENCE2019, Sofia 2-4 October 2019. ISIJ Digital Transformation, Cyber Security and Resilience, ISSN 0861-5160 (print), ISSN 1314-2119 (online), vol. 43, no. 1 (2019): 113-120, 2019, p.113-p.120 https://doi.org/10.11610/isij.4310

- Citation 1: Wang, Z., Guan, X., Zeng, Y., Liang, X. and Dong, S., “Utilizing data platform management to implement “5W” analysis framework for preventing and controlling corruption in grassroots government”. Heliyon Volume 10, Issue 7, 15 April 2024, e28601, DOI: 10.1016/j.heliyon.2024.e28601, 2024 (Scopus referenced: https://www.scopus.com/pages/publications/85188751354)
-

Конференции

- International Conference on Big Data, Knowledge and Control Systems Engineering BdKCSE'2018, (21-22 November 2018), доклад: “Unified innovative Platform for administration and automated management of internationally recognized standards”
- DIGILIENCE 2019: Digital Transformation, Cyber Security and Resilience Central Military Club Sofia, Bulgaria, October 2-4, 2019, доклад: “The logical model of unify, innovative Platform for Automation and Management of Standards (PAMS)”

Проекти

Част от изследванията в дисертационния труд са от проект № BG161PO003-1.1.06–0036-C0001 “Унифицирана платформа за администрация автоматизация и управление на международно признати стандарти”, изпълняван в сътрудничество от екипите на **Перфект Плюс ЕООД (ръководител Тодор Велев) и ИИКТ – БАН (ръководител Светозар Маргенов).** Проектът е за индустриално изследване на високотехнологичен иновативен продукт в областта на информационните технологии с продължителност 22 месеца.

Голяма част от резултатите са апробирани в проект „Разработка и въвеждане в експлоатация на Единна система за управление, контрол и анализ на дейностите (ЕСУКАД) за нуждите на Българския институт по метрология (БИМ)“, ръководен от Тодор Велев.

Благодарности

Изказвам своята благодарност на научният си ръководител проф. д-р Нина Добринкова, за ценни напътствия, професионална компетентност и съдействие при подготовката на дисертационния труд. Благодаря за помощта и съветите на колегите от ИККТ на БАН и от Solent University Southampton .

Приложения

Приложение 1 Основна терминология в стандартизацията
Приложение 2 Сертификационни (одитиращи) организации
Приложение 3 Изследване на данните
Приложение 4 Актуалност и промяна на документите и управление на записите.
Приложение 5 UML код на модела (Plant UML)
Приложение 6 Реализация на Платформата с Python
Приложение 7 ORM (Object-Relational Mapping) реализация – SQL Alchemy

Съдържание